Atty. Docket No.
005313.00001

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Of: Marc D. Van Heyningen

U.S. Pat. App. No.: 09/782,593

Filed: February 12, 2001

For: Method And Apparatus For Providing Secure Streaming Data Transmission Facilities Using Unreliable Protocols

Examiner: L. Son

Group Art Unit: 2135

REQUEST FOR RECONSIDERATION OF THE FINAL OFFICE ACTION DATED JULY 3, 2006

Commissioner for Patents
P.O. Box 1450,
Alexandria, Virginia 22313-1450

Sir:

Applicant respectfully asks for reconsideration of both this application and the final Office Action dated July 3, 2006.

In that Office Action, claims 1-3, 5-8, 10, 12-20, 22-28, 30-36, 38-43, and 45-48 were rejected under 35 U.S.C. § 102(e) over U.S. Patent No. 6,351,539 to Djakovic. Applicant respectfully traverses this rejection, and courteously asks for its reconsideration.

Claims 1-3, 5-8, 10, 12-15, 23-28 and 38-42 recite a method of transmitting data securely over a computer network that includes the steps of encrypting and transmitting data records. Claims 1-3 and 5-8 further recite that each data record incorporates a nonce and encrypted text that has been encrypted using the nonce. Claims 10 and 12-15 similarly recite using [a] corresponding nonce to encrypt text and incorporating the encrypted text and the corresponding

nonce into the data record, while claims 23-28 recite encrypting data records using a nonce such that each data record incorporates the nonce and text that is encrypted…using the incorporated nonce. Claims 38-42 then recite using [a] corresponding nonce to encrypt text, and appending the encrypted text and the corresponding nonce to the data record. Thus, each of these claims specifically recites that a data record includes both a nonce and text encrypted using the nonce.

This feature is not taught or suggested by the Djakovic patent. In making this rejection, the Examiner suggested that the random number generated by the random number generator 14 discussed in the Djakovic patent is the equivalent of the recited nonce. In particular, the Examiner stated:

> "(2) encrypting and transmitting data records between the first computer and the second computer using a reliable communication protocol, wherein each data record incorporates a nonce (RNG) and encrypted text that has been a encrypted using the nonce without reference to a previously transmitted data record" in (Col 4:1-25, and Col 5:50) (*a nonce is a random number. Djakovic teaches that random number generator is a true random sequence generators (Col 5 lines 35-44), which have the property that the generator's [s]equences cannot be reproduced, even with the same input. Therefore, the random number here used to encrypt the data record can not or will not have any reference to a previously transmitted data*) (See Office Action, page 3, lines 2-7, *emphasis in original*.)

The system disclosed in the Djakovic patent, however, does not incorporate the random number generated by the random number generator 14 into the data record, as expressly recited in claim 1-3 and 5-8. Instead, as discussed in, e.g., column 4, lines 1-18,

> The sequence of random numbers SR produced by the RNG 14 are combined with the enciphered output values S1 using XOR mechanism 24 to produce a second sequence of output values…input to the block cipher BC2 20 which operates on it (in encyrpting mode) using the 128-bit key K2 to produce a sequence of 64-bit output values (denoted S3). That is, S3=BC2(S2,K2).

> The sequence SR of random numbers produced by the RNG14 is also input to block cipher BC3 22 which uses the 256-bit key K3 (in encrypting mode)to produce an enciphered random sequence of 64-bit values (denoted SER=BC3(SR, K3)).

Thus, the output of the random number generator 14 is never even output from the cipher mechanism 10 for inclusion in a data record. Further, the value SER eventually output from the cipher mechanism is different from the output of the random number generator 14 (i.e, SR) applied in an XOR function against the ciphertext S1.

With particular regard to claims 6 and 34, these claims further recite verifying, for each received data record, that the incorporated nonce has not previously been received in a previously transmitted data record. This feature also is not taught or suggested by the Djakovic patent. In rejecting this claim, the Examiner has referred to the disclosure in the Djakovic patent that, with a true random number generator, the sequences created by the generator cannot be reproduced. (See Office Action, page 4, lines 9-15, referring to the Djakovic patent at column 5, lines 35-44.) This portion of the Djakovic patent does not, however, teach or suggest verifying that a nonce has not been previously received. Further, this portion of the Djakovic patent would actually teach away from this feature of the invention recited in claim 6. By teaching that a true random number generator cannot reproduce a sequence, the Djakovic patent would discourage one of ordinary skill in the art from verifying that a nonce has not previously been generated.

Regarding claims 7 and 27, each of these claims recites subject matter generally relating to the use of an indicator in a data record, and then processing the data record based upon whether the indicator was present. These features likewise are not taught or suggested by the

Djakovic patent. In rejecting this claim, the Examiner has referred to column 4, lines 1-25 and column 7, lines 32-45 of the Djakovic patent. Applicant respectfully points out, however, that both of these passages are silent with respect to any use of an indicator in a data record that will determine how the data record is processed.

With regard to claims 16-20 and 22, these claims recite a system for securely transmitting data using an unreliable protocol that includes a second computer having a communication protocol client function. These claims further recite that the communication protocol client function encrypts text for a data record using a nonce…and incorporates the respective encrypted text and nonce in the data record. As discussed in detail above, the Djakovic patent does not teach or suggest this feature of the invention.

Claim 19 additionally recites that the communication protocol client function is compatible with the SOCKS communication protocol, while claim 20 recites that the communication protocol client function is compatible with the SSL/TLS communication protocol. In rejecting both of these claims, the Examiner referred to column 6, lines 35-60 of the Djakovic patent. Applicant respectfully notes, however, that this portion of the Djakovic patent does not mention either the SOCKS communication protocol or the SSL/TLS protocol. Accordingly, it is courteously urged that this portion of the Djakovic patent does not, in fact, support the Examiner's rejection.

Claim 22 then recites subject matter generally relating to the use of an indicator in a data record, and then processing the data record based upon whether the indicator was present. These features likewise are not taught or suggested by the Djakovic patent.

Applicant thus respectfully submits that the Djakovic patent does not teach or suggest the features of the invention recited in any of claims 1-3, 5-8, 10, 12-15, 23-28 and 38-42. It is therefore requested that the rejection of these claims be reconsidered as well.

Next, the Examiner rejected claims 9, 11, 21, 29, 37 and 44 under 35 U.S.C. §103 over the Djakovic patent in further view of U.S. Patent Publication No. 2002/0101848A1 to Lee. Applicant respectfully traverses this rejection, and asks for its reconsideration as well. As discussed in detail above, the Djakovic patent does not teach or suggest the features of the invention recited in any of claims 9, 11, 21, 29, 37 or 44, and the Lee patent publication does note remedy the deficiencies of the Djakovic patent. Accordingly, Applicant urges that no combination of the Djakovic patent and the Lee patent publication could teach or suggest the features of the invention recited in claims 9, 11, 21, 29, 37 and 44, and therefore ask that the rejection of these claims also be withdrawn.

Lastly, the Examiner rejected 49-67 over the Djakovic patent in view of U.S. Patent No. 5,673,319 to Bellare et al. Applicant courteously traverses this rejection, and asks for its reconsideration.

Applicant first respectfully submits that one of ordinary skill in the art would not have been led to combine the teachings of the Djakovic patent and the Bellare et al. patent in the manner suggested by the Examiner. Both the Djakovic patent and the Bellare et al. patent are directed toward sophisticated techniques for encrypting text. The Bellare et al. patent, in particular, teaches the generation of a message authentication code (MAC), which is then used as an initialization vector. (See, e.g., column 5, lines 9-15.) In making this rejection, the Examiner

vaguely argued that

> Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Djakovi's invention to incorporate Bellare's CBC-MAC teaching to further authenticate each cipher block. (See final Office Action, page 10, lines 13-15.)

The Examiner has not explained, however, just how a new value, such as a message authentication code (MAC), might be incorporated into the specific encryption technique disclosed in the Djakovic patent without destroying it. Further, the Examiner has provided no reason or basis to argue that somehow including a message authentication code (MAC) into the encryption technique disclosed in the Djakovic patent would actually further authenticate each cipher block. Accordingly, Applicant submits that the Examiner has not set forth an actual *prima facie* showing of obviousness that would sustain the rejection of claims 49-67 over the combination of the Djakovic and Bellare et al. patents.

In any case, Applicant respectfully submit that no combination of the Djakovic and Bellare et al. patents would teach or suggest the features of the invention recited in any of claims 49-67. Each of these claims recites that a data record includes both a nonce and text encrypted using the nonce. As discussed in detail above, this feature is not taught or suggested by the Djakovic patent. Further, the Bellare et al. patent does not remedy this omission of the Djakovic patent. Accordingly, it is courteously urged that no combination of the the Djakovic and Bellare et al. patents would teach or suggest the features of the invention recited in any of claims 49-67.

In summary, Applicant submits that the Examiner has not set forth the *prima facie* showing of obviousness required to sustain the rejection of claims 49-67 over the combination of

the Djakovic and Bellare et al. patents. Further, Applicant courteously urges that no combination of the Djakovic and Bellare et al. patents would teach or suggest the features of the invention recited in claims 49-67. It is therefore requested that the rejection of these claims be withdrawn as well.

In view of the above remarks, Applicant respectfully submits that all of the claims are allowable, and that this application is therefore in condition for allowance. Applicant thus courteously asks for favorable action in this regard at the Examiner's earliest convenience.

Respectfully submitted,

By: s/Thomas L. Evans/s
Thomas L. Evans, Reg. No. 35,805

BANNER & WITCOFF, LTD.
1001 G Street, N.W., 11th Floor
Washington, D.C. 20001-4597
Telephone: (202) 824-3000
Facsimile: (202) 824-3001

Date: October 3, 2006